BAB 1
PENDAHULUAN

1.1. Latar Belakang

Perkembangan Teknologi Informasi (TI) saat ini berkembang secara pesat, baik dari sisi kecepatan maupun kemudahan masyarakat dalam mengakses informasi yang dibutuhkan. Sebelum era informasi, manusia merupakan sumber daya yang utama, dimana hampir semua pekerjaan dilakukan dengan tenaga manusia. Selanjutnya sumber daya modal memiliki peranan penting dalam menunjang kehidupan manusia. Seiring dengan kemajuan zaman, saat ini informasi telah menjadi sumber daya yang sangat penting bagi manusia. Jika dulu untuk mengirimkan satu berita membutuhkan waktu hingga berhari-hari dan membutuhkan biaya yang cukup besar, namun saat ini dalam hitungan detik berita itu sudah sampai dan tentunya dengan biaya yang lebih murah. Kehadiran era informasi diikuti dengan semakin berkembangnya kebutuhan masyarakat atas informasi. Perkembangan dunia maya adalah salah satu bukti dari perkembangan informasi dan teknologi dimana melahirkan internet sebagai sebuah fenomena dalam kehidupan manusia.

Menurut Mary Meeker dalam kompas.com edisi mei 2013 mengungkapkan bahwa pengguna internet di seluruh dunia telah mencapai angka 2,4 miliar orang pada mei 2013. Angka tersebut meningkat 8 persen dari tahun sebelumnya. Penggunaan internet dari perangkat *mobile* (*gadget*) juga terus meningkat drastis. Menurut Meeker pengguna internet *mobile* sudah menyentuh angka 15 persen dari keseluruhan lalu lintas internet dan akan melonjak hingga 30

persen pada akhir tahun 2014. Ini menunjukan bagaimana teknologi memang sudah menjadi kebutuhan dan gaya hidup manusia.

Segi positif dari perkembangan teknologi informasi tentu saja menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Disatu sisi TI dapat memberikan manfaat yang sangat berarti, mempermudah dan mempercepat akses informasi yang kita butuhkan mulai dari hal sederhana hingga dapat mengubah model perekonomian dan cara orang berbisnis. Namun dampak negatif pun tidak bisa dihindari. Seiring dengan perkembangan teknologi internet, menyebabkan munculnya kejahatan baru yang disebut dengan *cybercrime* atau kejahatan melalui jaringan internet. Munculnya beberapa kasus *cybercrime* di Indonesia, seperti pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program komputer.

Berkembangnya teknologi canggih dan sistem transfer dana elektronik (EFTS: *Electronik Funds Transfer System*) diikuti pula dengan berkembangnya kejahatan teknologi canggih (*hight tech crime*). Dikenal antara lain istilah cybercrime, EFT *crime, cybankcrime, internet banking crime, online business crime, hight tech wcc (white collar crime*), *bank fraud, credit card fraud, insurance fraud, stock market fraud, investment related fraud, online fraud* dan sebagainya.

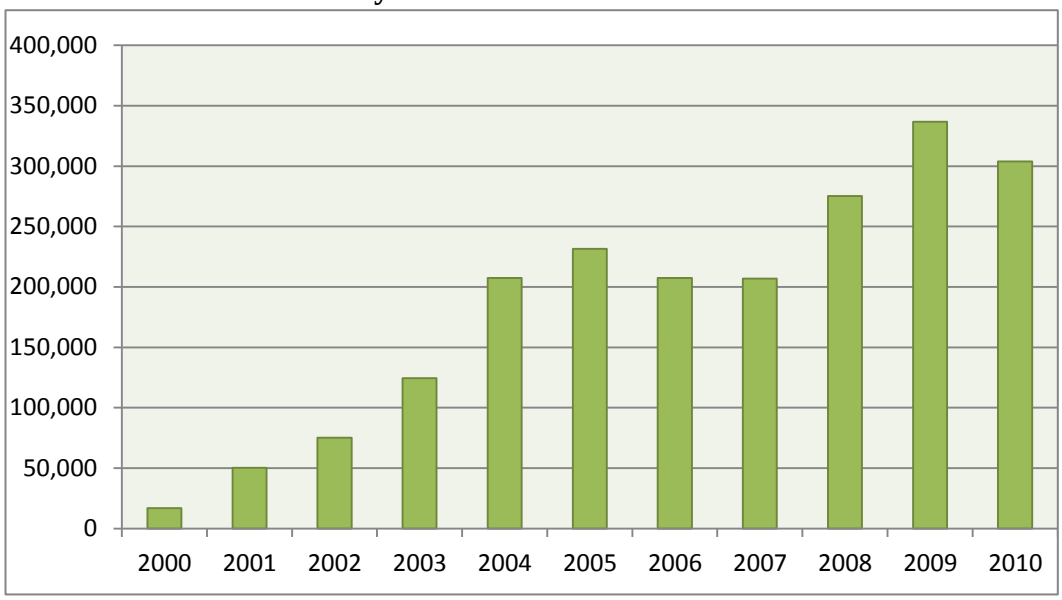
Kejahatan di dunia maya atau yang lebih dikenal dengan *cybercrime* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau

jaringan komputer yang menjadi alat, sasaran atau tempat terjadinya kejahatan. Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" (2013) mengartikan *cybercrime* sebagai kejahatan di bidang komputer yang secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.

Menurut Barda Nawawi Arief (2006:01) *cybercrime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Volodymyr Golubev dalam penelitian Heru Soepraptomo (2010) menyebutnya sebagai *the new form anti-social behavior.* Beberapa sebutan lainnya yang cukup fenomenal mengenai *cybercrime* antara lain sebagai kejahatan dunia maya (*cyber space/virtual space offence*), dimensi baru dari *high tech crime*, dimensi baru dari *transnational crime*, dan dimensi baru dari *white collar crime*. Cybercrime merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini.

Berdasarkan data dari *Internet Crime Complain Centre* (IC3) yang bekerja sama dengan FBI USA *(Federal Bureau of Investigation)* selama tahun 2010 di USA terjadi 303.809 kasus terkait *cybercrime*. Hal ini dapat dilihat pada data berikut :

Grafik 1.1.
Data Cybercrime di USA Tahun 2000 – 2010



(Sumber : *Internet Crime Complain Centre*)

Dari grafik diatas, terlihat tren yang ada selalu meningkat dari tahun ke tahun mulai dari tahun 2000 sampai dengan tahun 2010. Ini menunjukan pertumbuhan kasus *cybercrime* terus meningkat. Puncaknya terjadi pada tahun 2009 dan 2010 dimana jumlah kasus *cybercrime* mencapai angka diatas 300.000 kasus.

Tabel 1.1
Data Persentasi Jenis Cybercrime di USA Tahun 2013

No.	Jenis Cybercrime	Persentasi
1.	*Non-delivery payment / merchandise*	14,4 %
2.	*FBI- Related scam*	13,2 %
3.	*Identity theft*	9,8 %
4.	*Computer crime*	9,1 %

5.	*Miscellaneous fraud*	8,6 %
6.	*Advance fee fraud*	7,6 %
7.	*Spam*	6,9 %
8.	*Auction Froud*	5,9 %
9.	*Credit card fraud*	5,3 %
10.	*Overpayment fraud*	5,3 %

(Sumber : *Internet Crime Complain Centre*)

Pada tabel jenis *cybercrime*, dari data tersebut yang paling banyak terjadi adalah kasus *non-delivery payment* yakni sebesar 14,4%. Untuk kasus kejahatan kartu kredit menempati posisi yang cukup rendah hanya sebesar 5,3%. Namun hal ini terbalik dengan kondisi di Indonesia, dimana jenis kejahatan kartu kredit menjadi salah satu yang paling tinggi untuk kasus *cybercrime*.

Tabel 1.2.
Provinsi Teratas dalam Jumlah dan Tingkat Kejahatan di Indonesia
Tahun 2003

Provinsi	Peringkat kerawanan	Jumlah (Total Crime)	Tingkat (Crime Rate)	% dari Seluruh Indonesia
DKI Jakarta	1	37.895	228	19%
Jawa Timur	2	26.347	74	13%
Sumatra Utara	3	17.530	154	9%
Jawa Barat	4	17.188	48	9%
Jawa Tengah	5	12.528	36	6%

(Sumber : Pusdalop-Mabes Polri)

Tabel diatas menggambarkan tingkat kerawanan di lima provinsi yang menduduki peringkat teratas di Indonesia untuk tahun 2003. Kolom *Crime Rate* menunjukan jumlah kejahatan untuk setiap 100.000. Selama tahun 2003 diketahui bahwa DKI Jakarta paling rawan tindak kejahatan dengan total kasus mencapai 37.895 kejadian dan resiko kemungkinan mengalami tindak kejahatan mencapai 228 orang per 100.000 penduduk.

Berdasarkan koran tempo edisi mei 2013, statistik kejahatan dunia maya di Ibu Kota Jakarta sendiri pada tahun 2011 tercatat kerugian akibat *cybercrime* mencapai Rp 4 miliar dan US$ 178.876,50 dengan 520 kasus. Pada 2012, jumlah kasusnya meningkat menjadi 600 kejadian dengan kerugian Rp 5 miliar dan US$ 56.448. Pada 2013, sepanjang Januari-Maret, kerugian masyarakat sudah mencapai sekitar Rp 1 miliar. Frekuensi laporan masyarakat atas kejahatan jenis tersebut sebanyak 3-4 laporan per hari dibandingkan dengan 2012 yang hanya 2-3 laporan per hari.

Amerika Serikat dan negara-negara maju lain di dunia yang memiliki kelengkapan sistem dan lembaga-lembaga pengawas yang sangat kredibel dan efektif mampu dibobol oleh para *cybercrime*. Kondisi di Indonesia tentu sangat jauh lebih buruk dari Amerika Serikat. Kejahatan di dunia maya mulai masuk dalam ranah perusakan sistem perekonomian bangsa indonesia.

Menurut perusahaan keamanan Symantec dalam *Internet Security Threat Report* volume 17, Indonesia menempati peringkat 10 sebagai negara dengan aktivitas kejahatan *cyber* terbanyak sepanjang tahun 2011 lalu. Hal ini tak lain

disebabkan oleh terus meningkatnya jumlah pengguna internet di Indonesia. Bahkan Indonesia masuk lima besar pengguna jejaring sosial terbanyak di dunia.

Berdasarkan penelitian Symantec disebutkan juga bahwa Indonesia tercatat menempati peringkat 6 di dunia untuk kategori program jahat *spam zombie.* Padahal pada 2010 lalu, Indonesia masih menempati peringkat 28 untuk *spam zombie.* Para penjahat yang menyebarkan *spam zombie* dapat mengendalikan sebuah nomor telepon seluler di *smartphone* untuk menyebarkan SMS premium, demi mendapatkan keuntungan finansial. Sementara untuk kasus pencurian data dan informasi, Indonesia bercokol di posisi 27 setelah tahun 2010 lalu menempati urutan ke 30.

Kejahatan-kejahatan yang ditimbulkan oleh pelaku *cybercrime* telah merugikan dalam jumlah besar bagi korban dari pelaku *cybercrime*. Seperti pemberitaan mengenai kasus *cybercrime* yang terjadi di perbankan dimana terjadi pembobolan nasabah Bank BII yang mencapai Rp 21 Miliar dimana mengakibatkan kepanikan di tengah masyarakat. Kejadian itu membuktikan bahwa sistem pengamanan perbankan yang masih lemah sehingga dapat ditembus oleh pelaku *cybercrime.*

Teknologi informasi dibuat dalam rangka untuk mendukung dan meningkatkan kualitas informasi. Teknologi informasi yang aman dan baik diharapkan dapat meningkatkan kualitas atas laporan keuangan. Untuk menjaga kualitas laporan keuangan itu tetap baik perlunya suatu upaya pencegahan dan

penanganan khusus terhadap kejahatan-kejahatan TI sehingga dapat meminimalisir kejahatan-kejahatan tersebut.

Menurut Albrecht W. Steve untuk meminimalisir kejahatan tersebut dapat dilakukan dengan tiga cara yakni pencegahan, pendeteksian dan penginvestigasian. Upaya pencegahan merupakan salah satu langkah yang penting karena untuk meyakinkan bahwa sistem itu harus dibangun dengan pengendalian, baik itu yang bersifat *physical access* maupun *logical access.* Audit atas pengendalian *physical access* dilakukan melalui evaluasi atas pengamanan akses fisik ke lokasi pusat data dan sistem alarm untuk akses tanpa otorisasi pengamanan fisik lain terhadap hardware. Sedangkan audit atas pengendalian *logical access* dapat dilakukan dengan mengevaluasi kesesuaian otorisasi ataupun password dengan penetapan tanggung jawab (*job description*). Salah satu upaya pencegahan tersebut dilakukan dengan yang namanya audit atas teknologi informasi.

Secara umum audit teknologi infomasi adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal. Audit TI lebih dikenal dengan istilah EDP Audit (*Electronic Data Processing*), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer, yaitu audit melalui komputer dan audit dengan komputer.

EDP Audit telah mengalami perkembangan yang pesat. Perkembangan Audit TI ini didorong oleh kemajuan teknologi dalam sistem keuangan. *American*

Institute of Certified Public Accountants (AICPA) ikut mendukung pengembangan EDP Audit. Pada tahun 1977 edisi pertama *Control Objectives* diluncurkan. Publikasi ini kemudian dikenal sebagai *Control Objectives for Information and Related Technology* (CobiT). Dan pada tahun 1994, EDPAA mengubah namanya menjadi *Information System Audit* (ISACA).

Dalam PSA No. 60 [SA Seksi 314] disebutkan bahwa : "Penentuan risiko dan pengendalian intern – pertimbangan dan karakteristik sistem informasi komputer (SIK = penggunaan komputer dalam pengolahan informasi keuangan suatu entitas yang signifikan bagi audit, terlepas apakah komputer tersebut dioperasikan oleh entitas tersebut atau oleh pihak ketiga)". Ini menerangkan bahwa Sistem Informasi Komputer (SIK) memiliki peranan yang sangat penting dalam penentuan risiko dan pengendalian intern pada suatu entitas terutama dalam perbankan.

Persepsi untuk mengukur efektivitas metode pencegahan terhadap tindakan kejahatan didunia maya atau *cybercrime* merupakan persepsi dari auditor sistem informasi sebagai individu yang memiliki sikap independen. Hal ini untuk menjaga obyektivitas dari persepsi yang diberikan karena auditor sistem informasi merupakan elemen dari sistem informasi teknologi akuntansi.

Penelitian yang dilakukan oleh Heru Soepraptomo dalam jurnal penelitiannya "Kejahatan Komputer dan Cyber Serta Antisipasi Pengaturan Pencegahannya Di Indonesia" mengatakan bahwa dalam menghadapi perkembangan kejahatan siber yang melibatkan berbagai pihak dengan jurisdiksi

teritorial, waktu, hukum, negara, pemerintahan, sistem yang berbeda, memang masing-masing pemerintah atau negara harus tanggap, apakah masih dapat diselesaikan dengan hukum nasional yang berlaku, atau perlu pembaharuan dengan adanya konvensi internasional.

Hal yang membedakan penelitian ini dengan penelitian-penelitian sebelumnya, pada penelitian ini penulis menggunakan metode penelitian kualitatif dengan menggunakan data primer dan Auditor Sistem Informasi sebagai narasumber utama. Auditor Sistem Informasi merupakan orang yang khusus menangani audit sistem informasi. Sehingga data dan informasi yang didapat nantinya diharapkan dapat membuat hasil penelitian ini menjadi lebih baik dan dapat memberikan gambaran mengenai pencegahan tindakan *cybercrime* secara komprehensif.

Penelitian mengenai *cybercrime* di indonesia belum banyak dilakukan. Dari uraian latar belakang diatas terlihat bahwa fenomena kejahatan *cybercrime* di terus meningkat seiring dengan kemajuan teknologi informasi. Berdasarkan hal-hal tersebut di atas, maka penulis tertarik untuk melakukan penelitian mengenai **"Analisis Persepsi Auditor Sistem Informasi Mengenai Pencegahan Dalam Tindakan *Cybercrime*.**

1.2. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah bagaimana persepsi auditor sistem informasi mengenai upaya pencegahan atas tindakan *cybercrime* ?

1.3.Maksud Dan Tujuan Penelitian

1.3.1. Maksud Penelitian

Penelitian ini dimaksudkan untuk memperoleh informasi serta mengetahui persepsi dari auditor sistem informasi mengenai pencegahan atas tindakan *cybercrime*.

1.3.2. Tujuan Penelitian

Tujuan penelitian menurut Suharsimi Arikunto (2002:52) yaitu "Rumusan kalimat yang menunjukkan adanya sesuatu hal yang diperoleh setelah penelitian". Tujuan dalam penelitian berfungsi untuk menentukan arah pencapaian suatu permasalahan dalam penelitian. Tujuan penelitian penulis adalah untuk mengetahui bagaimana persepsi auditor sistem informasi mengenai upaya pencegahan atas tindakan *cybercrime*.

1.4. Kegunaan Penelitian

Setiap hasil penelitian yang dilakukan haruslah berguna serta mengandung unsur manfaat baik secara teoritis maupun praktis, khususnya bagi penulis dan pihak lain yang membutuhkan informasi dari hasil penelitian ini. Adapun manfaat atau kegunaan penelitian ini antara lain :

1.4.1. Kegunaan Teoritis

Penelitian ini diharapkan dapat memberikan wawasan di bidang audit sistem informasi dan tentang pencegahan kejahatan di dunia maya. Sehingga nantinya dapat menjadi bahan pembelajaran dan acuan bagi mahasiswa yang akan melakukan penelitian pada bidang yang sama.

1.4.2. Kegunaan Praktis

1. Bagi penulis

   Sebagai bahan pengembangan pengetahuan, wawasan, keterampilan dalam penulisan karya ilmiah serta melakukan penelitian khususnya mengenai pencegahan terhadap tindakan *cybercrime*.

2. Bagi Dunia IT

   Penelitian ini dapat digunakan sebagai bahan kajian dan masukan untuk pencegahan terhadap kejahatan-kejahatan didunia maya baik di indonesia maupun diluar negeri.

3. Bagi auditor Sistem Informasi

   Penelitian ini dapat menjadi bahan masukan bagi auditor Sistem Informasi dalam pengetahuan mengenai tindakan kejahatan didunia maya (*cybercrime*).

4. Bagi Kepentingan Dunia Akademik

   Hasil penelitian ini diharapkan dapat meningkatkan pengembangan kajian dan memberikan sumbangan informasi bagi peneliti selanjutnya dan masyarakat pada umumnya dalam memahami tindakan pencegahan terhadap kejahatan didunia maya berdasarkan persepsi Auditor Sistem Informasi.